REMARKS

Claims 1-26 are pending, of which claims 1, 19, and 22 are independent method claims with independent computer program product claim 12 corresponding to independent method claim 1. As indicated above, by this paper claims 5, 8, and 18 have been canceled and claims 1, 2, 3, 9, 10, 12, 14, 19, 20, and 22 have been amended.[1]

The Office Action rejected the independent claims 1, 12, 19, and 22 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,081,900 to Subramaniam et al. ("*Subramaniam*"). The remaining dependent claims were rejected as either anticipated under 35 U.S.C. § 102(e) by *Subramaniam* or as unpatentable under 35 U.S.C. § 103(a) over *Subramaniam* in view "Wireless Application Protocol Wireless Transport Layer Security" by En ("*En*").[2]

Applicants' invention, as claimed for example in independent method claim 1, relates to a communications device of an external client establishing a secure connection over a public network to a private network without restricting the communications device to working through the private network. The method includes the external client establishing a connection with a virtual private network access server of the private network over the public network using the communication device, the virtual private network server providing the external client access to the private network as though the external client is part of the private network; providing security to the connection through a communication protocol that resides at or above a socket layer in a protocol stack the external client uses to communicate data; maintaining a session that uses the secure connection to communicate with the private network; and during at least a portion of maintaining a session that uses the secure connection, the communication device retaining the ability to establish a separate and distinct connection with another resource outside of the private network. Independent claim 12 recites similar limitations from the perspective of a computer program product.

Applicants' invention, as claimed for example in independent method claim 19, similarly relates to a communications device of an external client establishing a secure connection over a

---

[1] Support for the claim amendments can be found throughout the Specification, including at page 4, lines 1-8; page 15, line 20 – page 16, line 21; page 18, lines 10-15); and Figure 3.

[2] Although the prior art status of all cited art is not being challenged at this time, Applicants reserve the right to do so in the future. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status or asserted teachings of the cited art.

Page 11 of 16

public network to a private network without restricting the communications device to working through the private network. The method includes securely connecting to a virtual private network access server of the private network through a communication protocol that resides at or above a socket layer in a protocol stack that the external client uses to communicate data in order to retain the ability to establish a separate and distinct connection with a resource outside of the private network, the virtual private network access server providing the external client access to the private network as though the external client is part of the private network; and while securely connected to the virtual private network access server, a specific act of accessing the resource outside of the private network.

Applicants' invention, as claimed for example in independent method claim 22, relates to a server computer system within a private network establishing a secure connection with a communications device of an external client without restricting the communications device to working through the private network. The method includes a virtual private network access server within the private network facilitating the establishment of a connection with the external client over the public network, the virtual private network server providing the external client access to the private network as though the external client is part of the private network; and facilitating the providing of security to the connection through a communication protocol that resides at or above a socket layer in a protocol stack used to communicate data, wherein the secure connection is established while allowing the external client to maintain the ability to establish a separate and distinct connection directly with one or more external resources rather than having to route communication with the one or more external resources through the private network.

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." MPEP § 2131. That is, "for anticipation under 35 U.S.C. 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly." MPEP § 706.02. Applicants also note that "[i]n determining that quantum of prior art disclosure which is necessary to declare an applicant's invention 'not novel' or 'anticipated' within section 102, the stated test is whether a reference contains an 'enabling disclosure.'" MPEP § 2121.01. In other words, a cited reference must be enabled with respect to each claim limitation. During examination, the pending claims are given

Page 12 of 16

their broadest reasonable interpretation, *i.e.*, they are interpreted as broadly as their terms reasonably allow, consistent with the specification. MPEP §§ 2111 & 2111.01.

Subramaniam discloses a border server in order to allow external clients secure access to a secure network. Col. 3, ll. 11-25; Figure 3. The border server includes a URL transformer to modify non-secure uniform resource locators in data being sent from a target server to the client by replacing them with corresponding secure URLs to promote continued use of secure communication. Col. 3, ll. 35-39. For example, the URL transformer may replace instances of "http" which refer to locations inside the secure network by corresponding instances of "https" which refer to the same locations. Col. 3, ll. 39-43.

As noted in Applicants' prior response, *Subramaniam's* border server operates more like a reverse proxy server than a virtual private network access server. *See* Specification, p. 15, ll. 14-19. For example, if an external client using *Subramaniam's* border server established a connection with a secure network as though the external client is part of the secure network, there would be no need for *Subramaniam's* URL transformer. In other words, the purpose for *Subramaniam's* border server seems to be transforming internal URLs to make them suitable for external clients—not to make it as though the external clients are part of the secure network.

In characterizing virtual private networks, *Subramaniam* indicates that previous approaches, including virtual private networks, to providing clients outside a secure network perimeter with secure access to Web pages stored on servers within the secure network have used strong encryption but have required that special software be previously installed on both the client machine which is seeking access and on the server machine which holds the data sought by the client. Col. 2, ll. 36-41 & 49-56. According to *Subramaniam*, these approaches protect user authentication information and/or the data which is transmitted after a user is authenticated, but they are not sufficiently convenient and efficient. Col. 2, ll. 56-59. In particular, *Subramaniam* indicates that virtual private networks require significant administrative effort and vigilant attention to details in order to avoid problems arising from incorrect or inconsistent configurations and that widely used Web browsers do not normally include full support for either virtual private networking or application-level encryption software. Col. 2, ll. 60-67.

In other words, *Subramaniam* confirms that virtual private networks have taken a distinct approach to security that *Subramaniam* characterizes as not fully supported by widely used Web browsers, such as those available from Netscape and Microsoft. *Subramaniam's* solution to

Page 13 of 16

providing convenient, efficient, and secure access to Web pages within a secure network is a border server acting much like a reverse proxy server. While one aspect of Applicants invention seeks to solve a similar problem, Applicants' solution is distinct—the use of a communication protocol that resides at or above a socket layer of a protocol stack in connection with a virtual private network access server. In addition to providing secure access to a private network using a virtual private network access server, Applicants allow for retaining the ability to establish a separate and distinct connection with a resource outside of the private network. This latter benefit, the ability to establish a separate and distinct connection with a resource outside of a private network when using a virtual private network access server to access a private network, is not even recognized by *Subramaniam*, much less solved.

Among other things, therefore, and in connection with the other recited limitations, *Subramaniam* fails to teach or suggest establishing a connection with a virtual private network access server of a private network, over the public network using the communication device, the virtual private network server providing an external client access to the private network as though the external client is part of the private network, and providing security to the connection through a communication protocol that resides at or above a socket layer in a protocol stack the external client uses to communicate data, as recited in independent claims 1 and 12.

Similarly, *Subramaniam* fails to teach or suggest securely connecting to a virtual private network access server of a private network through a communication protocol that resides at or above a socket layer in a protocol stack that an external client uses to communicate data in order to retain the ability to establish a separate and distinct connection with a resource outside of the private network, the virtual private network access server providing the external client access to the private network as though the external client is part of the private network, and while securely connected to the virtual private network access server, accessing the resource outside of the private network, as recited in independent claim 19.

And likewise, *Subramaniam* fails to teach or suggest facilitating the establishment of a connection with an external client over a public network, with a virtual private network server providing the external client access to the private network as though the external client is part of the private network, and facilitating the providing of security to the connection through a communication protocol that resides at or above a socket layer in a protocol stack used to communicate data, wherein the secure connection is established while allowing the external

Page 14 of 16

client to maintain the ability to establish a separate and distinct connection directly with one or more external resources rather than having to route communication with the one or more external resources through the private network, as recited in independent claim 22.

Rather, *Subramaniam* discloses a border server that operates more like a reverse proxy server than a virtual private network access server. There is no mention of a communication protocol that resides at or above a socket layer of a protocol stack in connection with a virtual private network access server or of the ability to establish a separate and distinct connection with a resource outside of a private network when using a virtual private network access server to access a private network. In fact, with respect to virtual private networks, *Subramaniam* only discloses the use of special software previously installed on both the client machine and on the server machine, which presumably suffers from the very problem Applicants' claimed invention solves.
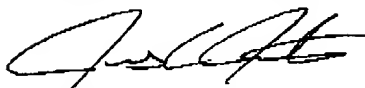
Based on at least the foregoing reasons, therefore, Applicants respectfully submit that the cited prior art fails to anticipate or make obvious Applicants invention, as claimed for example, in independent claims 1, 12, 19, and 22. Applicants note for the record that the remarks above render the remaining rejections of record for the independent and dependent claims moot, and thus addressing individual rejections or assertion with respect to the teachings of the cited art is unnecessary at the present time, but may be undertaken in the future if necessary or desirable, and Applicants reserve the right to do so.

In the event that the Examiner finds any remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney.

Application No. 09/768,673
Amendment "C" dated April 11, 2005
Reply to Office Action mailed January 27, 2005

Dated this _27_ day of April, 2005

Respectfully submitted,

RICK D. NYDEGGER
Registration No. 28,651
JENS C. JENKINS
Registration No. 44,803
Attorney for Applicant
Customer No. 47973

EMK:ahm
AHM0000000744V001

Page 16 of 16